IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS

In re Patent Application of: **KURDZIEL ET AL.**	)	
Serial No. **10/780,848**	)	Examiner: **A. NOBAHAR**
Filing Date: **FEBRUARY 18, 2004**	)	
Confirmation No. **2513**	)	Art Unit: **2132**
For: **CRYPTOGRAPHIC DEVICE AND ASSOCIATED METHODS**	)	Attorney Docket No. **RF-235 (50589)**

PRE-APPEAL BRIEF REQUEST FOR REVIEW

MS AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Responsive to the final Office Action of April 16, 2008, and in connection with the Notice of Appeal filed concurrently herewith, please consider the remarks set out below.

REMARKS

Applicants would like to thank the Examiner for the thorough examination of the present application, and for the courtesies extended during the telephone interview on October 7, 2008. The telephone interview focused on the "diffuser" as recited in the independent claims. The Examiner clarified that the "diffuser" in the cited prior art reference of Kanda et al. corresponds to the combining part **346** as illustrated in FIG. 5. The arguments supporting patentability of the claims are provided below.

I. The Claimed Invention

The present invention, as recited in independent Claim 1, for example, is directed to a cryptographic device comprising

an input stage, and an intermediate stage connected to the input stage. The input stage receives an input data block and a key data block comprising a plurality of sub-key data blocks, and generates a plurality of first signals therefrom that are in parallel. The intermediate stage comprises a plurality of substitution units operating in parallel, each substituting data within a respective first signal. A diffuser is connected to the plurality of substitution units for mixing data to generate a diffused signal. The diffuser comprises at least one shift register and at least one look-up table associated therewith. An output stage is connected to the intermediate stage for repetitively looping back the diffused signal to the input stage for combination with a next sub-key data block.

Independent Claim 10 is directed to a communication system comprising a key scheduler and a cryptographic device connected to the key scheduler, and is similar to independent Claim 1.

Independent Claim 18 is directed to a method for converting an input data block into an output signal in a cryptographic device, and is similar to independent Claim 1.

II. The Claims Are Patentable

The Examiner rejected independent Claims 1, 10 and 18 over the Kanda et al. patent. Kanda et al. is directed to a data transformation device for use in an encryption device of a secret key encryption algorithm that encrypts or decrypts data blocks using a secret key.

The Examiner referenced FIGS. 1, 2, 4 and 5 in Kanda et al. as disclosing the claimed invention. The Examiner characterized the input stage **17** illustrated in FIG. 2 as generating a plurality of first signals that are in parallel.

Still referring to FIG. 2, the plurality of substitution units operating in parallel (S-boxes S_0-S_7) is characterized as the intermediate stage, with each S-box substituting data within a respective first signal. The Examiner characterized block **346** illustrated in FIG. 5 as the diffuser connected to the plurality of substitution units S_0-S_7 for mixing data to generate a diffused signal.

The Examiner characterized FIG. 4 in Kanda et al. as disclosing an output stage connected to the intermediate stage for repetitively looping back the diffused signal to the input stage for combination with a next sub-key data block. In particular, the Examiner characterized that each of the round processing 38_0-38_{N-1} provides an output to the next one of the processing parts for combining with another subkey data block. The Examiner characterized that the round processing 38_0-38_{N-1} corresponds to the repetitively looping back.

In the claimed invention, the diffuser comprises at least one shift register and at least one look-up table associated therewith. The Examiner stated in the Advisory Action that Kanda et al. discloses an apparatus that performs logical linear transformation (which corresponds to the shift register) using substitution boxes and the linear transformation parts are constructed in memory as transformation tables (which corresponds to the look-up table).

The Examiner is correct to note that Kanda et al. discloses shift registers and look-up tables, but this is with respect to non-linear transformations. In particular, the non-linear transformation part 343_0-343_3 and the non-linear transformation part 345_0-345_3 as illustrated in FIG. 5 of Kanda et al. all include shift registers and look-up tables (i.e., transformation tables).

As discussed during the telephone interview, the Examiner clarified that the combining part **346** as illustrated in FIG. 5 is the diffuser. As also discussed during the interview, Kanda et al. fails to disclose that the combining part **346** includes a shift register and a look-up table for mixing data to generate a diffused signal. Instead, the combining part **346** merely combines the outputs from the non-linear transformation part **345_0-345_3** without mixing the outputs therefrom. Reference is directed to column 14 of Kanda et al., which provides:

> "As depicted in FIG. 5, these pieces of data mid_{10}, mid_{11}, mid_{12} and mid_{13} are then nonlinearly transformed in the nonlinear transformation parts **345_0**, **345_1**, **345_2** and **345_3** into the data out_0, out_1, out_2 and out_3, respectively, which are combined into the single piece of data Y_i * in the combining part **346**. Finally, the data Y_i * is linearly transformed into the data Y_i by, for example, a k_{i2} - bit left rotation in the third key-dependent linear transformation part **347** using the key data k_{i2}, thereby generating the output data Y_i from the nonlinear function part **304**. The nonlinear transformation parts **343_0** to **343_3** and **345_0** to **345_3** function just like S-boxes for DES cipher, and they are constructed by, for example, ROM, which receives input data as an address to read out therefrom the corresponding data." (Emphasis added).

As highlighted above, elements **345_0-345_3** non-linearly transform the respective data. Kanda et al. discloses that the non-linear transformation parts **345_0-345_3** function as S-boxes, as also highlighted above. The combining part **346** merely combines the outputs from the non-linear transformation part **345_0-345_3** without mixing the outputs therefrom.

Accordingly, it is submitted that independent Claim 1 is patentable over Kanda et al. Independent Claims 10 and 18 are similar to independent Claim 1. Therefore, it is submitted that these claims are also patentable over Kanda et al.

In view of the patentability of independent Claims 1, 10 and 18, it is submitted that the dependent claims, which include yet further distinguishing features of the invention are also patentable. These dependent claims need no further discussion herein.

III. CONCLUSION

In view of the arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,

MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
Telephone: 407/841-2330
Fax: 407/841-2343
Attorney for Appellant